HTTP

1. **Was ist HTTP?**

* HTTP-Protokoll in Webadressen
* Konzept von HTTP
* Zusammenhang mit HTML und URI

1. **Bedeutung von HTTP**

* HTTP steht für Hypertext Transfer Protocol
* Entwickelt von Tim Berners-Lee am CERN
* Verlinkung von Dateien durch Hypertext

1. **Zweck von HTTP**

* Kommunikation zwischen Webbrowser und Webserver
* Anforderung von Webseiten und Ressourcen
* Sprache des Webbrowser-Webserver-Austauschs

1. **Funktionsweise von HTTP**

* Schrittweise Erläuterung anhand eines Webseitenaufrufs
* HTTP-Request vom Browser zum Webserver
* Serverantwort mit Header und Message Body
* Darstellung der Webseite im Browser

1. **Verwendung von HTTP**

* Ursprüngliche Verwendung zur Anforderung von HTML-Dokumenten
* Vielfältige Anwendung in modernen Webseiten und Anwendungen
* Anfrage von Text, Bildern, Videos, Programmcode, Updates usw.
* Einsatz in REST-APIs, WebDAV, Machine-to-Machine-Kommunikation usw.

1. **HTTP-Versionen**

* Übersicht der verschiedenen HTTP-Versionen
* Entwicklungsgeschichte von HTTP

1. **HTTP/1**

* Urversion von HTTP
* Einfaches Abrufen von HTML-Dateien
* Verbindungs- und zustandslose Eigenschaften

1. **HTTP/1.1**

* Erster offizieller Standard von HTTP
* Medienunabhängigkeit und Cache-Mechanismen

1. **HTTP/2**

* Weiterentwicklung von HTTP zur Beschleunigung des Seitenaufbaus

1. **HTTP/3**

* Zukunftsaussicht für HTTP
* Aufbau auf dem UDP-Protokoll und QUIC
* Ziel der Vermeidung von "Head-of-Line Blocking"

SMTP

1. **SMTP - Simple Mail Transfer Protocol**

* Kommunikationsprotokoll für die Übertragung von E-Mails zwischen E-Mail-Clients und SMTP-Servern
* Mail Transfer Agents (MTAs) verwenden SMTP zur Kommunikation untereinander

1. **E-Mail-Routing über SMTP und DNS**

* SMTP-Server ist für das Weiterleiten von E-Mails an den Ziel-SMTP-Server verantwortlich
* DNS verwendet Mail Exchange Records (MX-Records), um den Ziel-SMTP-Server für eine Domain zu identifizieren
* Ablauf des E-Mail-Routings über SMTP und DNS
* Risiken von Mail-Schleifen bei unvollständigen oder falsch konfigurierten MX-Records

A picture containing diagram, screenshot, line, font

Description automatically generated

1. **Nachteile von SMTP**

* Keine automatische Versandbestätigung für gesendete E-Mails
* Unzustellbare E-Mails enthalten oft unverständliche Fehlermeldungen in englischer Sprache
* Fehlende Benutzerauthentifizierung führt zu gefälschten Absenderadressen und Spam-Missbrauch
* Maßnahmen gegen Missbrauch von SMTP-Servern sind optional und müssen aktiviert werden

1. **Aufbau einer E-Mail**

* Envelope: Sender-Adresse und Empfänger-Adresse für die MTAs
* Header: Informationen über den E-Mail-Client und die Message-ID
* Body: Nachrichten-Text der E-Mail

1. **Beispiel einer E-Mail**

* Darstellung einer E-Mail mit Return-path, Envelope-to, Received, Message-ID, From, To, Subject, Date und weiteren Headern

1. **SMTP-Status-Code**

* 3-stellige Status-Codes mit Klartext-Meldungen als Antwort des SMTP-Servers auf die Kommandos des Clients

FTP

1. **Wofür braucht man das File Transfer Protocol?**

* Das File Transfer Protocol (FTP) ermöglicht die Übertragung von kompletten Dateien.
* Es dient dem Dateiaustausch zwischen Client und Server
* FTP bietet ein Dateimanagementsystem mit hierarchischer Verzeichnisstruktur.

1. **Wie funktioniert FTP?**

* FTP läuft auf der Anwendungsschicht des TCP/IP-Protokollstapels und arbeitet ähnlich wie HTTP mit entsprechenden Programmen zusammen.
* Spezielle FTP-Programme oder Browser können für die Dateiübertragung verwendet werden.
* Es werden zwei Kanäle geöffnet: ein Steuerkanal (Port 21) für Befehle und Statuscodes und ein Datenkanal für die eigentliche Übertragung.
* FTP unterstützt aktiven und passiven Modus zur Datenübertragung.

1. **Sicherheit bei FTP**

* Das ursprüngliche FTP wurde ohne Sicherheitsvorkehrungen entwickelt und überträgt alle Informationen unverschlüsselt.
* Es existieren zwei sicherere Varianten: FTPS (FTP über SSL/TLS) und SFTP (SSH File Transfer Protocol).
* FTPS nutzt SSL/TLS für verschlüsselte Datenübertragung, während SFTP die Secure Shell (SSH) für sichere Dateiübertragung verwendet.

**POP3:**

1. Übertragung von E-Mails vom Server zum Computer.

2. Verwendung der Ports 110 und 995 (SSL/TLS-Verschlüsselung).

3. Client-Server-Architektur für Verbindung, Verwaltung und Abruf von E-Mails.

**IMAP4:**

1. Verwaltung von E-Mails auf dem Server.

2. Verwendung der Ports 143 und 993 (SSL/TLS-Verschlüsselung).

3. Client-Server-Architektur für Verbindung, Verwaltung und Abruf von E-Mails sowie Manipulation von Ordnern und Suchen nach bestimmten E-Mails.

**TLS:**

1. Verschlüsselung der Kommunikation zwischen Client und Server.

2. Verwendung des Ports 443 (für HTTPS) und anderer Ports.

3. Client-Server-Architektur für sichere Kommunikation, Authentifizierung des Servers durch digitale Zertifikate und Handshake-Protokoll zum Aufbau einer sicheren Verbindung.

**SSH:**

1. Sichere Remote-Verbindung und Kommunikation zwischen Client und Server.

2. Verwendung des Ports 22.

3. Client-Server-Architektur für Authentifizierung des Clients, verschlüsselte und authentifizierte Verbindung über unsichere Netzwerke, und Durchführung von Befehlen und Datenübertragung.